STRATEGY RESEARCH PROJECT

THE ROLE OF THE INTELLIGENCE COMMUNITY IN PREPARING TO WIN THE INFORMATION WAR

BY

WILLIAM W. McCOLLUM
National Security Agency

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

THE ROLE OF THE INTELLIGENCE COMMUNITY IN PREPARING TO WIN THE INFORMATION WAR

by

William W. McCollum
National Security Agency

Michael J. Morin
Project Advisor.

U.S. Army War College
Carlisle Barracks, PA 17013

ABSTRACT

AUTHOR: William W. McCollum

TITLE: The Role of the Intelligence Community In Preparing to Win the Information War

FORMAT: Strategy Research Project

DATE: 10 April 1997 PAGES: 22 CLASSIFICATION: UNCLASSIFIED

Increasing reliance on information-based technology is not unique to the United States, but growing awareness of the vulnerabilities created by this reliance has focused attention on protecting our information and information systems, while the potential value of offensive information operations, particularly in peacetime, has been less fully explored. This paper examines the relationship between defensive and offensive information warfare, looks at the status of governing policies and doctrine, discusses the vital role of intelligence in winning the defensive and offensive information war, and makes recommendations regarding organizing the intelligence community to support the successful prosecution of the offensive information war.

TABLE OF CONTENTS

Increasing reliance on information-based technology is not unique to the United States, but growing awareness of the vulnerabilities created by this reliance has focused attention on protecting our information and information systems, while the potential value of offensive information operations, particularly in peacetime, has been less fully explored. This paper examines the relationship between defensive and offensive information operations, looks at the status of governing policies and doctrine, discusses the vital role of intelligence in winning the defensive and offensive information war, and makes recommendations regarding organizing the intelligence community to prosecute offensive information operations successfully.

WHAT IS INFORMATION WARFARE?

In What is Information Warfare? Martin Libicki came to three conclusions: first, there is less to information warfare than meets the eye; second, information warfare has no business being considered as a single category of operations; and third, most of what U.S. forces can usefully do in information warfare will be defensive, rather than offensive.[1]

In the eighteen months since Libicki reached these conclusions the U.S. defense community has made considerable progress in reaching agreement on what constitutes information warfare. Two key terms have been adopted to cover the actions taken in crisis during peacetime, conflict and war to achieve information superiority over an adversary. The first is *information operations*, which covers the actions taken to affect adversary information and information systems while defending one's own information and information systems. The second is *information warfare*, which applies to

information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. *Information superiority* is agreed to encompass the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.[2] What emerges from the definitions are the two inseparable aspects of information operations - defensive and offensive.

Within the Joint Chiefs of Staff responsibility for defensive information warfare lies with the J6, and the J3 is responsible for offensive information warfare. The common thread linking the two is the target sets both sides must consider - information and information systems. Whether the task is to defend or attack, there are five vital components of information that must be analyzed and accounted for in order to achieve the mission. These components are integrity, authentication, non-repudiation, confidentiality, and availability.

Information has integrity when both the sender and receiver are certain that it has not been altered in any way. Authentication in an information exchange guarantees that the sender and receiver are each sure of the identity of the other. Non-repudiation means that the information exchange includes a mechanism to ensure that neither participant can claim successfully not to have been a party to the exchange. Confidentiality means simply that the exchanged information was not divulged to an unauthorized recipient. Information is available when anyone with authorized access can retrieve it.[3]

The defender must establish a protected information environment, which assures access to timely, accurate, and relevant information wherever and whenever needed. Not only must the defender protect the environment and deter attacks, his defense must be

able to detect an attack, respond to it effectively, and restore the protected environment. An attack on an information system can be directed at one or more of the components.

THE QUESTION OF VULNERABILITY

In little more than a decade the United States has become dependent on networked information systems to conduct essential business, including military operations, government, and commerce. This networking has become a critical component of our competitiveness as a nation, making the information infrastructure that supports it a potential center of gravity of our national power.

The national security implications of the networking of America are not yet fully understood and appreciated among those who must defend the nation, much less among the public at large. But the fact is that our ability to network has far outpaced our ability to protect networks, and the increased efficiency of networking has come at the price of increased vulnerability to attack of information and information systems.[4] Information in unprotected or poorly protected networks can be accessed, changed, or destroyed. Unprotected systems can be controlled, damaged, or shut down. Through the interconnectivity offered by the Global Information Infrastructure, targeted systems can be attacked from almost anywhere in the world.

Employed on a large scale against a nation heavily reliant on unprotected networks, attacks on information and information systems have the potential to inflict massive levels of destruction on military readiness and on the economy. Despite official efforts, the United States is both heavily reliant and largely unprotected. The Defense and National Information Infrastructures offer minimal defense against unauthorized

access and use. This is of great concern to the defense community, since 95 per cent of DoD's peacetime communications are carried on the public switch network. At the very time when our conventional defenses have achieved unprecedented effectiveness, networking has offered our adversaries a way around them. It has opened a virtually unobstructed avenue of approach to our heartland over which an attacker, committing only modest resources, could achieve disruptive effects on a scale approaching that of a nuclear attack. The method of attack - offensive information warfare.

The need to protect vital information and information systems has been documented in a broad array of guidance documents from the National Security Strategy (NSS) to military service manuals. In the most recent National Security Strategy (NSS) under the heading "Enhancing Our Security," the writers note that, "...the threat of intrusions to our military and commercial information systems poses a significant risk to national security..."[5] In his March 1996 "Annual Report to the President and the Congress," Secretary of Defense William Perry captured the essence of the importance of information operations to the security of the nation when he said, "The enormous U.S. dependence on information and its supporting infrastructure simultaneously enables fielding and effective employment of the world's premier military force, and creates significant...vulnerabilities for the United States which DoD's Information Warfare initiatives are addressing."[6]

In the face of such a threat, it would not be surprising to learn that the development of an effective defense is foremost in the minds of those who are aware of the vulnerabilities. In fact, two major national efforts have been undertaken to determine the extent of the nation's vulnerability and to make recommendations to minimize the

risks. In October 1995 a Defense Science Board Task Force on Information Warfare was established under the direction of the Under Secretary of Defense for Acquisition and Technology and was charged with focusing on threats to Department of Defense information and information systems. In July of 1996 President Clinton signed Executive Order 13010 which established the President's Commission on Critical Infrastructure Protection to perform a similar assessment of certain national infrastructures, "...so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[7]

The Defense Science Board reported its findings in a November 1996 report described by the Wall Street Journal as "unusually strident."[8] It recommended more than three billion dollars of additional spending over the next five years to improve the security of the nation's telecommunications and computing infrastructure. Calling current Pentagon efforts inadequate, the panel made 13 recommendations including the creation of an "information warfare czar" within the Department of Defense and the establishment of an information warfare center within the U.S. intelligence community. Perhaps the most significant recommendation in the report was that the Pentagon be given the legal ability to repel and pursue those who try to hack into its computer systems.

The President's Commission is to report its findings as they are made and submit a final report not later than 15 July 1997. The vulnerabilities which gave rise to the creation of the commission are perceived to be so serious that the administration is not willing to wait for the commission's report before taking action. The executive order creating the commission also created an Infrastructure Protection Task Force to, "increase

coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact."[9]

WHY THE EMPHASIS ON DEFENSE?

Is there a real threat or are we merely crying wolf? The full potential of information operations has not been demonstrated, so how do we know that our infrastructure is vulnerable to this type of attack? We know both through test attacks against our own defense networks and through clear evidence that our vulnerabilities are being exploited today. The Defense Science Board Task Force concluded from its investigation that the current threat is significant, the vulnerabilities are numerous, and countermeasures are extremely limited.

In 1995 the Defense Information Systems Agency (DISA) demonstrated the vulnerability of DoD unclassified logistics, support, and medical networks.[10] Using techniques widely available to anyone with an interest, DISA experts attacked nearly 10,000 DoD computers, successfully gaining access to 88 per cent of them. Only four per cent of the successful penetrations were detected by the organizations under attack. Of those organizations detecting attacks, only five per cent reacted. Overall, during these tests only one in a thousand successful attacks drew an effective defensive response. Based on these results and the current level of reported security incidents, the number of penetrations of DoD systems in 1996 has been estimated in the hundreds of thousands.

There is evidence that the vulnerabilities noted in DISA's testing have been found and exploited by real-world attackers. In 1996 more than 250 unclassified DoD computer systems were known to have been penetrated by outsiders. Functions supported by these

systems included weapon and supercomputer research, logistics, finance, procurement, personnel management, payroll, and military health systems.[11] The incidence of such attacks is escalating and the number is projected to double in 1997. Even more ominous is a media report that Dutch hackers in 1990 penetrated U.S. military networks and obtained detailed information about military plans for DESERT SHIELD and DESERT STORM. They offered this information to Saddam Hussein, for a price, but the details were reportedly so extensive that Hussein believed it was fake.[12]

As recently as 20 March 1997 Duane Andrews, who chaired the Defense Science Board study, testified before Congress in open hearings that, "...unless the Pentagon - and the national government at large - is adequately prepared to deal with the information warfare threat, there is the prospect for an 'electronic Pearl Harbor.' "[13]

AREN'T OUR ADVERSARIES VULNERABLE, TOO?

Strategic Assessment 1996, prepared by the Institute for National Strategic Studies, notes that, "...the U.S. government needs to muster the full range of options at its command if it is to achieve its goals at a price consistent with the resources its citizens are prepared to devote to international affairs."[14] One of the emerging instruments of military power is offensive information operations, of which the Strategic Assessment says, "making potential aggressors know that the United States could abjure brute force but still wreak havoc on their societies would be a powerful new instrument of power."[15] This instrument would have applications across the full range of military operations. As a deterrent it could be used to remind a nation's leaders of their vulnerability. If deterrence fails, "...attacks on opponents' computers could undermine the advanced

sections of these opponents' economies, hinder the mobilization of military power, and put heavy pressure upon hostile leadership."[16]

Former Secretary of Defense William Perry, in his 1996 "Report to the President and the Congress," placed equal emphasis on defensive and offensive information operations when he stated that, "[information operations seek] to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, processes, and systems."[17]

The Chairman of the Joint Chiefs of Staff, General John Shalikashvili, reinforced the holistic view of information operations in Joint Vision 2010, which is "...the conceptual template for how America's Armed Forces will...leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[18] He asserted that the achievement of information superiority will require both offensive and defensive information operations and that efforts are underway in the defense community to develop nontraditional methods of both components.

WHAT IS THE STATUS OF INFORMATION OPERATIONS POLICY AND DOCTRINE?

Within the Department of Defense and the Joint Staff , the capstone directives and instructions on information operations deal extensively with defense against attacks, even though they acknowledge that the same technologies which create dependencies and vulnerabilities for the United States also create vulnerabilities for our adversaries that can be exploited using offensive information operations capabilities.

One of the earliest directives on the subject, Department of Defense Directive TS-3600.1, Information Warfare, was almost entirely oriented toward conflict and warfare in its original version from December 1992. A reissue of the directive in December 1996 had the stated purpose of updating information operations and information warfare policy, definitions, and responsibilities within the Department of Defense; however, a close examination of the new directive reveals a major shift in orientation. The title was changed to Information Operations, the goal of which, "...is to secure peacetime national security objectives, deter conflict, protect DoD information and information systems, and to shape the information environment."[19] Three of the four objectives are offensive in nature and are arguably peacetime goals.

With this jointly coordinated policy statement in place, the way was cleared for the development of a more offensively oriented joint doctrine statement, which appeared in draft form in January 1997. Joint Publication 3-13, Joint Doctrine for Information Operations, devotes a full chapter to offensive information operations and instructs combatant commanders to, "carefully consider the potential of information operations for deterring and rolling back crises."[20]

At about the same time the Director for Operations (J3) and the Director for C4 Systems (J6) of the Joint Staff published the brochure, Information Warfare: A Strategy for Peace...The Decisive Edge in War. The brochure treats defensive and offensive information operations as complementary and mutually supporting aspects of one vital mission area. This document also provides some insight into why offensive information operations doctrine has developed more slowly than defensive doctrine:

"Defensive information warfare activities are conducted on a continuous basis in both peacetime and war, and are an inherent part of force protection. Offensive information warfare capabilities may be employed in a variety of circumstances across the range of military operations. *Information warfare operations may involve complex legal and policy issues requiring careful review and national-level coordination and approval.*"[21]

CONCLUSIONS

In support of his contention that there is less to information warfare than meets the eye, Martin Libicki argued that, even though information systems are becoming more important, the vulnerabilities attributed to them can be managed if they are taken seriously. This will, in turn, minimize the value of trying to attack information systems. Even while Libicki was writing, serious efforts were underway to manage the vulnerabilities of information systems, but providing security for networked systems presents an unprecedented challenge. In the past, classified information moved over dedicated circuits and was stored and processed by stand-alone computers. In a networked world connection to anything means connection to everything. To fully utilize the capabilities of networked systems, users need the ability to manage and distribute data of different security sensitivities over common, public-switch networks. The United States is a world leader in defensive technologies, but even the U.S. is approaching the problem with a goal of risk management, not risk avoidance. This means that there will still be targets, albeit "hardened" ones, to be exploited.

Although the defense community has succeeded in agreeing on an information operations definition, information warfare is not considered to be a single category of operations. Supported by intelligence it encompasses efforts in six areas - defensive

information warfare, information attack, operational security (OPSEC) and deception, psychological operations (PSYOP), electronic attack, and physical destruction. The terminology *information warfare* describes an integrating strategy to target and protect information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems.

Clearly, defending U.S. information and information systems is a high priority, but the fact that these systems have vulnerabilities means that the systems of potential adversaries are also vulnerable. Libicki contended that information systems are more important to U.S. forces than they are likely to be to opposing forces, but an understanding of how an opposing force uses information to make decisions is a critical element in determining whether offensive information operations techniques can be used to advantage. Libicki also contended that the U.S. will not be able to do much of what is called offensive information warfare due to the rules of engagement that the United States will likely observe. As our understanding of the threat matures and our ability to counter it develops, rules of engagement across the full range of military operations will almost certainly evolve to allow the use of this new weapon.

As demonstrated above, protection of U.S. information systems requires detailed knowledge of their vulnerabilities and a robust research and development program to develop and field the hardware and software needed to minimize the risks. Successful exploitation of an adversary's information systems demands the same level of knowledge, as well as an understanding of how the adversary uses information to make decisions. The key to posturing the U.S. defense community to win the information war is to

organize the intelligence community so that it can gather the information necessary to both protect friendly systems and attack enemy systems.

Intelligence and information systems security have a long history of complementing each other. Intelligence provides an information advantage over our adversaries, while information systems security prevents others from gaining a comparable advantage over us. Together these functions offer information superiority for the United States.

The networking of America and the threat of information warfare have resulted in the requirement for a seamless integration of intelligence and information systems security. In the days of dedicated defense communications, security was deemed sufficient if the confidentiality of the information could be protected while the information was being transmitted. Today, when 95 per cent of defense communications are on the public switch network, confidentiality is not enough. The data must be protected from alteration and destruction and there must be assurance that the data exchanges are originated and received by valid participants.

This is a more active concept than simply encrypting information for transmission. Providing security in a large-scale information warfare scenario may involve sealing off or restricting access to critical segments of the communications infrastructure, either physically or cryptographically. In this environment information systems security will need help from intelligence. It will ask intelligence to answer two critical questions. Are we under attack and, if so, by whom?

Answering these questions would have been relatively simple in days gone by. Our intelligence system was finely tuned over a period of four decades against the threat

of a large-scale conventional attack in Europe and a strategic nuclear exchange. Not only was it capable of answering these questions, it could have given us indications and warning information about a potential attack. But the intelligence demands of information warfare are something new. We are just beginning to formulate the intelligence requirements this new threat brings with it.

Are we under attack? The DISA test cited earlier suggests that our capabilities to detect intrusions into our information systems are weak, at best. How far could a strategic campaign aimed at our critical information infrastructure progress before being recognized?

Who is attacking us? Unlike nuclear, conventional, chemical or biological warfare, information warfare requires little identifiable infrastructure. Information warfare forces are highly mobile, with individuals or small teams equipped with laptop computers capable of launching attacks from any point on the global network. Above all, information warfare is cheap, putting the capability within reach of most nations and many non-state actors such as terrorist groups and criminal cartels. These factors give information warfare a substantial degree of plausible deniability. Bringing force to bear to stop an attack will likely be slowed by the need to determine the identity of the attacker, and whether or not the attack is state sponsored or is the effort of a non-state actor.

The information warfare battlefield is unfamiliar terrain for both information systems security and for intelligence. In the near term information systems security will need to develop a more active defensive strategy, and intelligence will need to identify new threats, develop new sensors, and perhaps move into cyberspace in both a passive

and an active way. Information systems security will depend upon intelligence to tell them what is happening and, as capabilities mature, what is going to happen.

Over the long term both the scope and nature of information warfare will change as our potential adversaries acquire more sophisticated offensive capabilities. Information warfare will become global in scope as the United States and its allies and friends interact on the same Global Information Infrastructure as their avowed and potential adversaries.

These new offensive weapons will give our adversaries the capability to launch attacks against the U.S. information infrastructure from virtually any point on the globe with an INTERNET connection. Such attacks would be difficult to stop using our current geographically-based command structure and traditional weaponry. Cyberspace provides a vast and borderless hiding place into which to deploy information warfare weapons well in advance of an attack. It will likely become increasingly difficult to isolate and neutralize an opponent's information warfare capabilities using hard kill techniques against targets within the opponent's borders. While hard kill attacks will continue to play an important role in information warfare, it is possible that cyberspace will become information warfare's battlefield. Cyberspace may emerge as an Area of Responsibility (AOR) with its own weapons, tactics and intelligence requirements.

What will these new intelligence requirements look like? The answer will depend in large part on the defensive capabilities we are able to field. At present these are not robust. While we have developed techniques to provide for data integrity, authentication of users, non-repudiation assurance, confidentiality of data, and availability of service, deployment of these techniques has been constrained by resource limitations, leaving

gaps in our defenses. Further, these techniques provide minimal capability to detect and actively counter sophisticated information warfare attackers.

For now, given the current state of information systems security technology, defensive information operations require relatively modest intelligence support. This will change with the advent of more responsive and proactive information systems security techniques. As we begin to field capabilities permitting the conduct of active defensive operations in cyberspace, our intelligence organization for information warfare will need to support coordination between offense and defense, as well as support effective information warfare battle management. New defensive information operations concepts and capabilities will generate major new demands on the intelligence system.

RECOMMENDATIONS

If the intelligence community is to play a vital role in the future development of information warfare, the United States must develop a set of information operations capabilities that will allow both the gathering of intelligence from and about adversaries' information systems and the degradation, deception, or destruction of those information systems in crisis during peacetime, conflict, and war. These capabilities must include both equipment and expertise.

The development of these capabilities must take place in an integrated manner within both the intelligence community and the Department of Defense. There are several challenges to be met:

- in acquiring capabilities we must ensure that the organizations which develop information attack equipment, techniques, and expertise share their knowledge in a systematic way to avoid duplication of effort;

- in managing the collection of intelligence we must establish a procedure for tasking the collection of information needed to support information attacks;

- in authorizing information operations attacks we must establish a procedure that is both legal and timely for operations in peace, crisis, and war; the procedure must specify the respective roles of agencies and departments and must take into consideration the notification of Congress; and

- in controlling operations, we must establish procedures for the conduct of information attacks, including planning, coordination, assessment of gain vs. loss potential, decision-making authority; and evaluation of effectiveness.

Acquisition of the capabilities to conduct information operations activities is problematic and fraught with potential legal issues. The intelligence community and the military departments have programs to develop information systems attack capabilities. Many of these capabilities are dual use; that is, they permit entry into an information system both for the purpose of obtaining foreign intelligence and for degradation, destruction, and/or exploitation of the same system. There is an uneven exchange of information among the organizations developing these capabilities for their own purposes. A more integrated coordination mechanism is needed in order to build dual-use devices which meet the foreign intelligence requirements of intelligence agencies and can be turned to deterrence or warfighting if necessary.

The Defense Science Board Task Force on Information Warfare had it almost right when they recommended that an "information warfare czar" be named within the Department of Defense and that an information warfare center be established within the U.S. intelligence community. The "czar" should be responsible for information *operations* and the center should also include representatives from the military services to ensure that the research and development activities are compatible with the Command,

Control, Communications, Computers and Intelligence (C4I) systems in use by the wartime information warfare "trigger pullers."

The development of information operations intelligence collection requirements is central to building an effective information operations capability. The collection management system must address all potential sources of information and it must gather what a diverse set of users actually needs. The system must foster a dialogue among the information operations experts, military users, and non-military users such as counter-drug, counter-terrorist, and counter-crime officials. The collection management function should be part of, or collocated with, an intelligence community information warfare center so that it can understand both information operations technology and the intelligence needed to design defensive and offensive systems.

The authorization of information operations also requires the development of an appropriate structure. At the top of this structure should be an organization empowered to authorize the undertaking of *special information operations*, which are defined as information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process.[22] This should probably be done within the National Security Council and particular attention should be paid to the possibility of having to notify Congress under the War Powers Act.

Control of information operations is probably the most complex issue which must be addressed. The authorities for conducting information operations for foreign intelligence purposes lie within the intelligence community and are reasonably clear, although the fact that information systems are not tied to national boundaries could cause

problems. If an operation is to degrade, deceive, or destroy a foreign information system in peacetime it would be governed by the provisions of Executive Order 12333, with respect to covert action (CA).[23] The complexity arises when operations are conducted during a crisis, which could lead rapidly to conflict. The transition from CIA control of covert actions to military control of conflict requires close coordination. Here, too, there is a need for a structure to ensure that the relevant CINC is fully informed of CIA operations and that CIA is aware of CINC-controlled operations to prepare the battlefield. Perhaps this coordination could be accomplished by the National Intelligence Support Team (NIST) which would, in all likelihood, be deployed with the CINC or with the Joint Task Force Commander.

Whether or not information warfare represents a genuine revolution in military affairs will continue to be debated and the answer will come only in hindsight. What must be done now is to structure the defense and intelligence communities so that resources are expended wisely to ensure that the United States achieves information superiority.

ENDNOTES

[1] Martin C. Libicki, What is Information Warfare? (Washington: US Government Printing Office, 1995), 96-97.

[2] Department of Defense, Information Operations, DoD Directive S-3600.1 (Washington: US Department of Defense, 9 December 1996), 1-1.

[3] The Joint Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2nd Edition (Washington: The Joint Staff, 4 July 1996), B-69, 74-75.

[4] The Joint Staff, Information Warfare: A Strategy for Peace...The Decisive Edge in War (Washington: The Joint Staff, n.d.), 1.

[5] William J. Clinton, A National Security Strategy of Engagement and Enlargement (Washington: U.S. Government Printing Office, February 1996), 13.

[6] William J. Perry, Annual Report to the President and the Congress (Washington: US Department of Defense, March 1996), 236.

[7] William J. Clinton, Executive Order 13010, President's Commission on Critical Infrastructure Protection (Washington: 15 July 1996), 1.

[8] Thomas E. Ricks, "Information Warfare Defense is Urged," Wall Street Journal, 6 January 1997, sec. B, p. 1.

[9] William J. Clinton, Executive Order 13010, 4.

[10] Department of Defense, Defense Science Board Task Force on Information Warfare - Defense (Washington: US Department of Defense, November 1996), 2-15.

[11] *ibid.*

[12] "Hackers Offered Iraq U.S. Military Information," The Washington Post, 16 March 1997, p. B2.

[13] Bryan Bender, "Lawmakers Get Education on Perils of Cyber Warfare," Defense Daily, 94 (21 March 1997): NeWSprint 9305-1.

[14] Lt Gen Ervin J. Rokke, USAF, Strategic Assessment 1996: Instruments of U.S. Power (Washington: National Defense University Press, 1996), 195.

[15] *ibid.*

[16] *ibid.*

[17] Perry.

[18] General John M. Shalikashvili, Joint Vision 2010 (Washington: The Joint Staff, 1996), 1.

[19] Department of Defense, Information Operations, DoD Directive S-3600.1, 1-2.

[20] The Joint Staff, Joint Doctrine for Information Operations (Draft), Joint Pub 3-13 (Washington: The Joint Staff, 21 January 1997), II-16.

[21] The Joint Staff, Information Warfare: A Strategy for Peace...The Decisive Edge in War, 4.

[22] Department of Defense, Information Operations, DoD Directive S-3600.1, 1-2.

[23] Reagan, Ronald, Executive Order 12333, United States Intelligence Activities, (Washington: 4 December 1981), 3.

BIBLIOGRAPHY

Bender, Bryan. "Lawmakers Get Education on Perils of Cyber Warfare." Defense Daily, 94. NeWSprint 9305-1.

Clinton, William J. A National Security Strategy of Engagement and Enlargement. Washington: U.S. Government Printing Office, 1996.

_____Executive Order 13010. President's Commission on Critical Infrastructure Protection. Washington: 15 July 1996.

Department of Defense. Information Operations. DoD Directive S-3600.1. Washington: U.S. Department of Defense, 9 December 1996.

Department of Defense. Defense Science Board Task Force on Information Warfare - Defense. Washington: November 1996.

"Hackers Offered Iraq U.S. Military Information." The Washington Post, 16 March 1997, p. B2.

The Joint Staff. Information Warfare: A Strategy for Peace...The Decisive Edge in War. Brochure. Washington: The Joint Staff, n.d.

The Joint Staff. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington: The Joint Staff, 4 July 1996.

The Joint Staff. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington: The Joint Staff, 7 February 1996.

The Joint Staff. Joint Doctrine for Information Operations (Draft). Joint Pub 3-13. Washington: The Joint Staff, 21 January 1997.

Libicki, Martin C. What is Information Warfare? Washington: U.S. Government Printing Office, 1995.

Perry, William J. Annual Report to the President and the Congress. Washington: U.S. Government Printing Office, 1996.

Reagan, Ronald. Executive Order 12333. United States Intelligence Activities. Washington: 4 December 1981.

Ricks, Thomas E. "Information Warfare Defense Is Urged." Wall Street Journal, 6 January 1997, sec. B, p. 1.

Rokke, Ervin J., Lt Gen, USAF. Strategic Assessment 1996: Instruments of U.S. Power. Washington: National Defense University Press, 1996.

Shalikashvili, John M., Gen, USA. Joint Vision 2010. Washington: The Joint Staff, 1996.